U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

DEPARTMENTAL REGULATION	Number: 3170-001
SUBJECT: End User Workstation Standards	DATE: December 12, 2007
	OPI: Office of the Chief Information Officer

1. PURPOSE

The objectives of the United States Department of Agriculture's (USDA) End User Workstation Standards requirements are: (a) to ensure cyber security protection, (b) to increase effectiveness in acquiring and administering resources by promoting compatibility and interchangeability of workstation hardware and software, (c) to ensure that these standards are aligned with the enterprise architecture business goals and processes of USDA, and (d) to meet the policy requirements of OMB Circular A-130 and OMB policy memorandum M-07-11.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

This regulation will remain in effect until superseded. Appendices are forthcoming.

3. BACKGROUND

The Clinger-Cohen Act of 1996 (40 U.S.C. (11101 et seq.)), as amended by the Information Technology Management Reform Act (ITMRA) and OMB Circular A-130, "Management of Federal Information Resources", require Federal agencies to build and maintain a Profile of Standards and Technical Reference Model that supports IT investment management and development of enterprise architecture. More recently, the Office of Management and Budget issued policy memorandum M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," which stated: "agencies with these operating systems [Windows XP and VISTA] and/or plans to upgrade to these operating systems must adopt these standard security configurations by February 1, 2008." Established standards for workstation hardware and software are vital to ensure that USDA complies with these and other workstation mandates.

4. POLICY

This policy requires the agencies and offices under the administrative oversight of the Department of Agriculture to follow a set of standards regarding workstation computers. The Chief Information Officer of the USDA (CIO USDA) is required

to establish standards to ensure the cyber security of the agencies', Department, and Government-wide networks. These standards include hardware, operating systems, and applications.

The workstation standards are contained as appendices to this general policy. Each appendix is to be established within 90 days of the approval of this policy with comments from agencies, and reviewed quarterly in the first year of this policy. After the first year, a review of each of the appendices are to be conducted in the first month of the second quarter; reviewed for comment by the agencies for 30 days; and finalized prior to the end of the second quarter.

The USDA CIO is to ensure the following during the annual review:

a. support for the continuity of operations to the USDA programs;
b. focus areas and training maximizing the use of the standard workstation configuration;
c. centralized support of operating system and application patches to maintain the cyber security protection of over 130,000 workstations;
d. establishing an enterprise architecture standard;
e. meeting the workstation security requirements of the Office of Management and Budget;
f. achieving discounts by volume purchasing;
g. providing automated inventories through vendor information transfer;
h. supporting smartcard based security;
i. supporting the Department's thin client, mobile technology, and teleworking policy;
j. ensuring consistency to provide users better Tier 1 helpdesk service;
k. creating a functional workstation that will assist our employees with their daily work requirements; and
l. minimize the expense of workstation rotation and replacement.

Agencies and offices of the United States Department of Agriculture shall procure computer workstation hardware and software consistent with the standards identified in the appendices of this regulation. Exceptions to these standards may be requested through specific procedures identified in Paragraph 7 of this regulation.

The following appendices provide the detailed selection specifications for conforming to the policy requirements of this regulation:

a. Appendix A, "End User Workstation Hardware Standards"
b. Appendix B, "End User Workstation Security Standards"
c. Appendix C, "End User Workstation Software Standards"
d. Appendix D, "End User Workstation Peripheral Standards"

e. Appendix E, "USDA Conservation and Green Standard Requirements for Workstations"
f. Appendix F, "USDA Standards for Acceptable Disposal of Batteries and Other Workstation Components"
g. Appendix G, "Other Workstation Standards"

5. BENEFITS

The benefits to the Department, agencies, and users from the standardization of workstations include better security for the Government's networks, better helpdesk support, increased inventory management capabilities, support of USDA telework and mobile computing technologies, adherence to OMB workstation security requirements, lower operating costs, and volume based purchasing discounts.

USDA uses information technology (IT) to assist in achieving program objectives and reporting requirements. Consistency in USDA's IT allows the development of safe, efficient and cost-effective methods for supporting programs and in planning for upgrades, migrations, staff training, and future technology installations. In addition, these standards promote cross-agency information sharing, increase interoperability, and improve Departmental communication and collaboration.

6. RESPONSIBILITIES

a. The USDA CIO is:

(1) The final, approving authority on the adoption of IT standards to ensure the security of Government networks, maximize the benefit of technology purchases, and minimize investment and operating expense.

(2) The final reviewer and approver of exceptions to the workstation standard requested by the agencies or staff offices.

b. The Office of the Chief Information Officer (OCIO) will:

(1) Develop basic policies and standards for the end-user workstation environment.

(2) Provide management and oversight activities related to workstation operating system configurations, to include but not limited to:
(a) Providing periodic updates to all operating system configurations to ensure systems security posture is maximized;
(b) Reviewing and monitoring compliance with established operating systems policy;

(c) Testing all configurations in a non-production environment to ensure compatibility with legacy applications;
(d) Supporting the agencies by testing operating system software;
(e) Creating a software update architecture that is able to receive and approve patches and updates from the Department of Homeland Security for deployment to the USDA enterprise;
(f) Creating and maintaining a security configuration guide for each operating system; and
(g) Reporting compliance and deviations to OMB.

(3) Establish enterprise-wide contracts for standard hardware and software.

(4) Establish and maintain the green policy, recycle policy, and energy conservation policy for computer workstations, in accordance with applicable Government-wide policies and standards.

c. Department agencies and staff offices will:

(1) Adopt the policies and standards for the end-user workstation environment by:
(a) Establishing procedures and controls to ensure the use of these standards;
(b) Ensuring effective communication between local systems administrators and OCIO; and
(c) Incorporating these standards in each agency's and office's capital planning and investment control process.

(2) Implement and maintain operating system and security configuration settings by:
(a) Scanning and providing periodic updates to all operating system configurations to ensure systems security posture is maximized;
(b) Documenting all deviations from these standard operating systems settings with a detailed rationale for the deviations, and requesting a waiver from the Cyber Security Division in OCIO;
(c) Providing corrective action plans for the timely remediation of issues not authorized as an approved deviation;
(d) Ensuring only qualified and trained personnel are granted elevated privileges;
(e) Ensuring that elevated privileged accounts are not mail or Internet enabled;
(f) Ensuring all custom or commercial off the shelf (COTS) applications are written to be run as "user";
(g) Creating an authorized software list that includes all the software that can be used on these configurations; and

(h) Employing the use of the National Institute of Standards and Technology (NIST) Security Content Automation Protocol (S-CAP) tool to help evaluate providers and perform self evaluations.

(3) Procure standard hardware and software from enterprise–wide contracts as they are made available.

(4) Request acquisition of hardware and software using the Acquisition Approval Request (AAR) process prior to any procurement. The AAR must identify whether or not the acquisition of hardware or software to be procured meets the USDA standards, the contracts to be used and must provide a detailed rationale if the product(s) being purchased does not meet the standard, regardless of whether the standard is a product or a specification(s).

7. EXCEPTION REQUEST PROCESS

Some agencies may have special conditions or requirements that prevent full compliance with this regulation. Agencies may request a special exception by submitting written justification to the USDA CIO for review and decision. The justification must include the business reasons that show a different option is in the best interest of the agency and USDA for cyber security, technology development, and expense reduction. All requests must be signed by the Agency CIO.

The written exception request is to be in the form of a decision memorandum and is to include:

i. Indication of Request for Exception
ii. Name of submitting agency
iii. Name and contact information of submitting person
iv. Information technology description (hardware/software exception)
v. Justification to show good cause for the exception. The request should document the justifications for the exception and the impact of granting versus not granting the request.
vi. Cyber security management plan
vii. Technology development summary
viii. Technology refresh plan
ix. Cost justification
x. Signature of Agency CIO.
xi. Date of the request.

8. DEFINITIONS

a. Workstation. Desktop, laptop, or other computer used by the employee to complete their daily tasks.

b. Desktop Computer. A computer made for use on a desk in an office or home, and is distinguished from portable computers such as laptops or Personal Digital Assistants (PDA). Desktop computers are also known as microcomputers.

c. Laptop Computer. A small mobile computer, which usually weighs 2-18 pounds (1-6 kilograms), depending on size, materials, and other factors.

d. Thin Client. Server-centric computing hardware in which the application software, data, and CPU power resides on a network server rather than on the client computer.

-End-